⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－108277

⑤1Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和61年(1986)5月26日
H 04 N 7/167		7013－5C	
H 04 K 1/00		7240－5K	

審査請求　未請求　発明の数 1　（全6頁）

⑤4発明の名称　有料放送方式

㉑特　願　昭59－229017
㉒出　願　昭59(1984)11月1日

⑦2発明者　森田　博幸　深谷市幡羅町1－9－2　株式会社東芝深谷工場内
⑦2発明者　国井　満雄　深谷市幡羅町1－9－2　株式会社東芝深谷工場内
⑦1出願人　株式会社東芝　川崎市幸区堀川町72番地
⑦4代理人　弁理士　則近　憲佑　外1名

明　細　書

1. 発明の名称　有料放送方式

2. 特許請求の範囲

放送局側において、所定非公開鍵情報を用いて発生乱数が制御される乱数発生手段と、

この乱数発生手段に対する制御データとして機能する少なくとも各加入者に対応した非公開鍵情報を収納するデータメモリと、

この非公開鍵情報をもとに加入者の契約の有無を判別する契約判別手段と、

前記データメモリから読み出された非公開情報をもとにして前記発生手段に得られた乱数を用いて放送情報をスクランブルする手段とを有し、

加入者側において前記非公開情報を抽出する鍵抽出手段と、

この鍵抽出手段で抽出された鍵情報が当該加入者固有鍵情報と一致するか否かを判別してディスクランブル制御信号を発生する鍵復号手段と、

この契約者識別手段による識別結果に応じて前記乱数に対応した乱数を発生する乱数発生手段と、

この乱数発生手段で発生する乱数を用いてスクランブルされた放送情報をディスクランブルするディスクランブル手段と、

加入者契約時に視聴者が指定した加入者識別符号と加入者機器固有の非公開情報との整合を判別する加入者識別手段とを具備し、

加入者が番組予約するに際しては加入者識別手段によって指定された加入者の固有情報と加入者機器固有情報の整合を確認した上で予約を許可することで誤まった課金がなされることを防止することを特徴とする有料放送方式。

3. 発明の詳細な説明

〔発明の技術分野〕

この発明は、例えば放送衛星等を用いた空中線或は伝送線を介するＣＡＴＶに代表される有線形態で、映像、音声、データ、図形情報をサービスする形態において、視聴を契約した加入者のみにサービスを行なう有料放送方式に係り、特に契約加入者以外の者に対し視聴を阻止する制御を行なう有料放送方式に関する。

(1)　(2)

〔発明の概要〕

この発明は例えば第1図に示すように、放送局側では対象契約番組の種類を示す公開鍵としてのティア(Ti)とこれに対応する非公開情報としてのティアキー(Ki)をメモリテーブル60に収納し、また、メモリテーブル70には加入者識別符号(ID)を収納して上記ティアキー(Ki)、加入者識別符号(ID)とをもとにCPU100によって乱数発生器10を制御する。この乱数発生器10で発生する乱数によって有料放送情報は排他的論理和回路20でスクランブルされる。

一方、受信側においては、伝送された上記非公開鍵情報及び加入側200のROMに予じめ与えられている暗号情報等の非公開情報からの情報をもとに放送局側で発生した乱数と同様の乱数が乱数発生器で発生するようCPU300が制御する。この乱数を用いて排他的論理和回路210でディスクランブルを行なう。また、番組予約に際しては加入者識別信号をキーパッド500で入力するが、この場合ROM226に収納された加入者固有の符号と

この場合、有料放送方式において加入者が有送番組を予約するには識別符号(ID)とともに所望の番組を予約する訳であるが、実際の加入者以者の名義で不正予約を防ぐ意味において当該契約者固有の識別信号(ID)を放送局側に告知することを番組予約時に行なわせるシステムが採用される。即ち、識別信号(ID)、及び予約対象番組を示す公開鍵であるティヤ(Ti)と呼ばれる情報で放送局側に番組予約をし、放送局側ではこれらの公開情報を秘匿情報に変換してどの加入者が契約したかの情報及び信号に対するスクランブルを解くための情報の両者を秘匿する。この秘匿情報は加入者側に送られ、この秘匿情報より復号化鍵を生成し暗号化された情報を平文化して復号を行なう。

このような有料方式においては上記したように放送局側に対する番組予約は公開鍵を用いて行ない放送局側で課金に対する検査を行なった後に暗号化された情報を平文化するに必要な情報が加入者側にダウンロードされる。

上記有料放送方式においては加入者が放送局に

の照合を行ない照合結果によって予約処理が課金マップ90の情報を処理した後に上記メモリテーブル60の情報の内容の変更を行なう制御を行なう。

これにより、この発明に係る有料放送方式では誤まった予約情報によって課金がなされることを防止し得る。

〔発明の技術的背景とその問題点〕

近年、新放送メディアの発達にともない、テレテキスト、静止画放送、高品位テレビジョン放送、デジタル信号による多チャンネル放送が可能となってきている。このような放送メディアの高度化により放送番組の伝送種類も多岐にわたってきている。

そして、放送側においては特定番組に対して課金を行ない放送局側と契約を行なった特定の加入者以外の加入者に対しては伝送信号に対して攪拌を与え、いわゆるスクランブルを行ない視聴を阻止し、契約加入者に対してはこのスクランブルを解除することによって視聴を可能にする有料放送が有料番組に対して行なわれる。

対して番組予約等に代表されるアップストリームに対する処理は加入者識別信号をもとに行なわれる。従って、加入者は加入者自身に付された識別信号(ID)を放送局側に送った上で予約処理を行なうが、この場合上記加入者識別信号(ID)を加入者に認識させる有効な手段が必要とされる。

〔発明の目的〕

この発明は上記の点に鑑みなされたものであり有料システムにおいて、加入者識別信号(ID)等を加入者側の機器の固有の符号との照合を行なった上で加入者の番組予約を可能として不正視聴を防止できる有料放送方式を提供することを目的とする。

〔発明の実施例〕

以下、この発明の一実施例を図面を参照して説明する。

第2図はこの発明に係る有料放送方式の一実施例を示す回路図である。この第2図に示す回路によって放送信号に対するスクランブルよって伝送信号に対する暗号化がなされるが、課金対象とな

るデジタル放送情報は入力端子ＩＮに印加される。

この放送情報は有料放送としてスクランブル処理され加入者に対してのみ復号がなされるよう、乱数発生器20で発生した乱数を用いて排他的論理和回路20でスクランブル処理がなされる。この排他的論理和回路20の出力に得られるスクランブル化された放送情報は、契約加入者に対してのみ復号が許可されるが、復号のために必要な情報を放送局側100から加入者側200に伝送する必要がある。

上記したように、放送信号自体は上記擬似ランダム雑音を発生する乱数発生器10の動作により秘匿されるが、どの契約者にどのような番組の視聴を許可するかの復号可能契約者を特定する情報も秘匿する必要がある。このように、番組情報自体を秘匿するための秘匿鍵情報、復号可能契約者を特定するための秘匿鍵情報の２種の暗号鍵としての秘匿鍵情報により有料化がなされる。

このような有料放送システムにおいては、加入者を示す識別符号(ID)、及び予約番組の種類を示

キー(Ki)からなるメモリマップより抽出され上記乱数発生器10に与えられる。この結果、上記乱数発生器10は、上述の２種類の暗号鍵であるイニシャルデータ(In)、ティアキー(Ki)を用いてKs＝ｆ(In,Ki)なる乱数を発生する。この乱数Ksは一方入力端に放送情報が加えられる排他的論理和回路20の他方入力端に加えられスクランブル化された放送情報が得られる。

この場合、上記イニシャルデータ(In)は、スクランブル化された放送情報を平文化するため暗号鍵情報として用いられるので、イニシャルデータ自体も加入者側にダウンロードされる。

放送局側では、どの加入者がどの番組に対して契約しているかの情報を暗号文として生成するがこの情報もダウンロードして加入者側での復号のための鍵情報(Ei)として用いられる。この暗号情報Eiはメモリテーブル70に形成された各加入者を識別する識別符号(ID)に対応して付された秘匿情報であるパスワード(Pa)と上記ティアキー(Ki)とにより Ei＝g(Ki,Pa) として暗号器80で生成されるティア(Ti)の公開鍵情報、上記乱数発生器10に対する初期値(In)、上記ティア(Ti)に対する暗号符号であるティアキー(Ki)、上記識別符号(ID)に対応するパスワード(Pa)が非公開の暗号鍵として扱われる。

先ず、放送情報を秘匿化する乱数発生器10について述べると、この乱数発生器は例えばＭ系列符号発生器等で構成され所定のアルゴリズムによる乱数が発生する。この場合乱数発生器10の初期値は同期信号発生回路30で発生するタイミング信号にもとずき、制御回路40の制御のもとにイニシャルデータ発生回路50によって発生する。このイニシャルデータ(In)は上記ティアキー(Ki)とあいまり上記乱数発生器10のシーケンス動作を制御する。

即ち、上記乱数発生器10のシーケンス動作は上記イニシャルデータ(In)とティアキー(Ki)によって制御を受けるわけであるが、上記ティアキー(Ki)は、メモリテーブル60に形成されたチャンネル番号毎に付され番組ジャンルを示すティア(Ti)及びこのティア(Ti)に対して付された暗号ティア

る。暗号情報(Ei)も加入者側でスクランブルされた放送情報を復文化するため鍵情報として用いられるので、この暗号情報(Ei)を復号できない加入者はスクランブルされた放送情報をディスクランブルして放送信号を受信することはできない。従って課金マップ90をＣＰＵ110が参照し、ＣＰＵ110は料金未納等の契約対象外の者に対しては上記暗号情報(Ei)を作成せず当該加入者は放送の視聴が禁止される。

このように放送局側100からは、第１の鍵情報Ksでスクランブルされた放送情報、契約加入者を特定するに供する第２の鍵情報Ei、及び上記乱数発生器10に対する初期値情報(In)がタイミング回路120によるタイミング制御のもとにモデム130を介して秘匿情報として加入者側120にダウンロードされる。更に、公開鍵である番組態様を示すティア(Ti)がダウンロードされる。

次に、加入者側200についてみると、スクランブルされた放送情報は排他的論理和回路210の一方入力端に加えられる。このスクランブルを解く

には、上記乱数発生器10で発生した乱数と同じ乱数を上記排他的論理和回路210の他方入力端に加えればよいが、この復号化は上述した第1の鍵情報Ksと、第2の鍵情報Eiを生成して乱数発生器220でスクランブル時における乱数と同様の乱数を発生することで行なわれる。このようなディスクランブルに供する乱数を発生するには上記第1の鍵情報を生成する必要があるが、加入者側では第1の鍵情報Ksを再生するためにはティアキー(Ki)、イニシャルデータ(In)を抽出することが必要になる。この場合、ティアキー(Ki)は、ダウンロード時に第2の鍵情報Eiで暗号化されているためティアキー(Ki)を直接抽出できず一担第2の鍵情報(Ei)を抽出しこれからティアキー(Ki)を抽出する処理が行なわれなければならない。

ディスクランブル動作を説明するに、先ずデータ処理に必要な同期信号は同期信号抜取り回路221によって抽出され、この同期信号をもとにデータ処理に必要なタイミング信号をタイミング信号発生回路222が発生する。また、放送局側100

00

復号器231は上記RAM225から読み出した鍵情報(Ei)と上記ROM226から読み出した加入者に付されたパスワード(Pa)から上記暗号器80と逆のデータ処理を行ないティアキー(Ki)を生成する。このティアキー(Ki)及び上記鍵情報抽出回路288で抽出したイニシャルデータ(In)をもとに乱数発生器220でスクランブルに供する乱数と同様の乱数が発生する。この乱数は排他的論理和回路210に加えられ、ディスクランブル処理がなされ平文化された放送情報を出力端子OUTに得る。

これらの一連のディスクランブルに関連するデータ処理はCPU300による制御による。

次に、契約加入者側200から加入者が放送局側100に対して契約を申し込む場合について述べる。

加入者が契約するには、先ず表示器400に表示された加入者識別符号(ID)をキーパッド400を押釦して入力する。この後、加入者は予じめ知らされている番組態様を示すティア(Ti)を上記キーパッド500を操作して入力し、番組予約を行なう。これらの加入者識別符号(ID)、ティア(Ti)はCP

03

から送られた関連鍵情報は鍵情報抽出回路223で抽出される。即ち、イニシャルデータ(In)、鍵情報Ei=g(Ki,Pa)、及びティア(Ti)が鍵情報抽出回路233で上記タイミング発生回路222で規定されるタイミングに従がい抽出される。この抽出された関連鍵情報はRAM書込制御回路224の制御信号の制御によってRAM225に書き込まれる。このとき、各加入者毎に付されている加入者識別符号(ID)、及びパスワード(Pa)が加入者側のROM226から読み出されたものと一致しているか否かを比較器227で判別し、比較の結果一致しているときのみ上記RAM225に対し関連鍵情報の書き込みが許可される。

また、イニシャルデータ(ID)、公開鍵情報である番組態様を示すティア(Ti)は鍵情報抽出回路228で抽出され上記RAM225に書き込まれたティア(Ti)と伝送された番組に付随するティア(Ti)との比較を比較器229で比較を行ない、この比較の結果ティアが一致している場合には制御回路230によって復号器231を動作させる。このとき

02

U300で処理された後にモデム600を介してアップストリームによって放送局側へ送られる。放送局側100では上記加入者からの予約情報である加入者識別符号(ID)、ティア(Ti)はモデム130で復調された後、課金マップに加入者識別符号(ID)をもとに課金情報を書き込む。そして、CPU110は上記課金マップ90を参照し、料金支払い等を確認した後にメモリテーブル60に対して非公開情報であるティアキー(Ki)を書き込む。これにより予約処理が行なわれ、放送局側100から有料放送情報を入力端子INから送出する場合には排他的論理和回路20によってスクランブル処理が行なわれた信号が伝送され、加入者側200では契約加入者のみ排他的論理和回路210によってディスクランブルされる。

このように加入者が契約するにあたっては加入者識別符号(ID)と希望する番組態様に対応した情報であるティア(Ti)を放送局側100に送るわけであるが、この発明にあっては当該が入者以外の名義で不正に番組が予約され、未契約者が不正に視

04

聴することを防止する機能を有する。

即ち、加入者が契約するには希望番組の態様に応じたティアキー(Ki)の指定にともない加入者固有の加入者識別符号(ID)をキーパッド500の押釦によって指定させることで他人の識別符号(ID)を用いて契約することを防止する。

これは、契約時にキーパッド500を押釦して指定した加入者識別符号(ID)と当該加入者機器内の固有ROM226に書き込まれた加入者識別符号(ID)が一致しているか否かをCPU300で判別しこの判別の結果両者が一致していないとモデム600の変調動作を停止することで放送局側100に予約情報が伝達されるのを禁止する。この結果、メモリテーブル60にティアキー(Ki)が書き込まれず、加入者側でディスクランブルするに必要とされる前述した鍵情報 Ei＝(Ki,Pa) が放送局側で形成されないので鍵情報(Ki)が当該加入者側200にダウンロードされず当該加入者による不正視聴は阻止される。

つまり、CPU300のレジスタ301に加入者特

るようにして上記メモリテーブル60に対してティアキー(Ki)の書き込みを制御してもよい。

このように、加入者側200での加入者の契約に際して、加入者固有の識別符号(ID,パワード)を用いて契約を許可して上記課金マップ90への課金情報の書換えがなされるので加入者識別符号を誤まって指定しても他の加入者への課金が誤まってなされることが防止できる。

〔発明の効果〕

以上述べたようにこの発明によれば、加入者自体が正しく加入者識別信号(ID)を入力しない限り契約が許可されないので、誤まって他人の加入者識別符号(ID)をもとに番組を予約してもアップストリームを介して予約情報は放送局側で処理されず当該他人に対して誤まって課金がなされることのない有料放送方式を提供し得るものである。

また、第3者が不正に他人の加入者識別符号(ID)を用いて番組契約を行なっても当該契約が許可されず不正な有料番組の視聴が阻止できる有料放送方式が提供される。

有の加入者識別信号(ID)をROM226から読出し一方加入者がキーパッド500から入力した加入者識別符号(ID)との比較をコンパレータ303で比較し比較の結果一致している場合には、キーパッド500を用いて入力した加入者識別信号(ID)及びティア(Ti)はアップストリームに伝送することがスイッチ(SW)が閉成されることにより許可される。

このようにして加入者識別符号(ID)を加入者側機器で照合し、この照合結果にもとずき上記モデム600を制御することによってディスクランブルの解除を阻止して有料放送の不正視聴が妨げられる。この場合、上記加入者識別符号(ID)の照合の結果上記モデム600を制御した例を述べたが、結果的に上記メモリテーブル60に対するティアキー(Ki)の書き込みの禁止がなされる制御がなされれば上記の実施例に限られるものではない。

また、上述の例にあっては加入者側における番組契約時においては契約の許可を加入者識別符号をもとに行なったが、加入者側において上記ROMから読み出したパスワード(Pa)を利用して照合す

更に、上述の実施例では加入者はモデム600を介して予約情報として加入者識別符号(ID)、ティア(Ti)をアップストリームを介して伝達する例を示したが、この発明はこれに限られず上記予約情報を電話等を介して放送局側100に伝達する形態であってもよい。

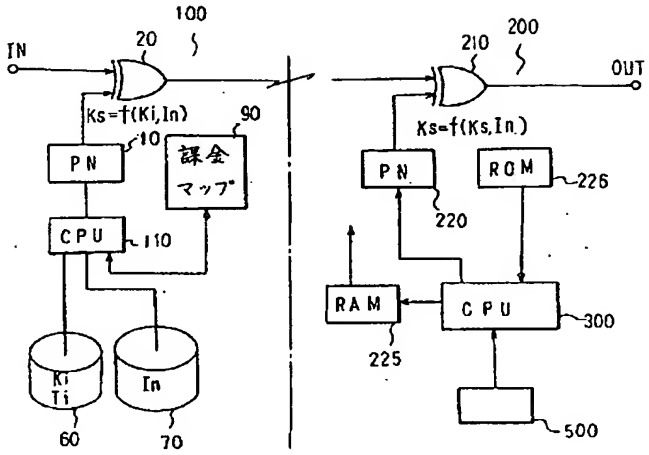
4. 図面の簡単な説明

第1図はこの発明に係る有料放送方式の実施例の概要を示す回路図、第2図はこの発明に係る有料放送方式の実施例を示す回路図である。

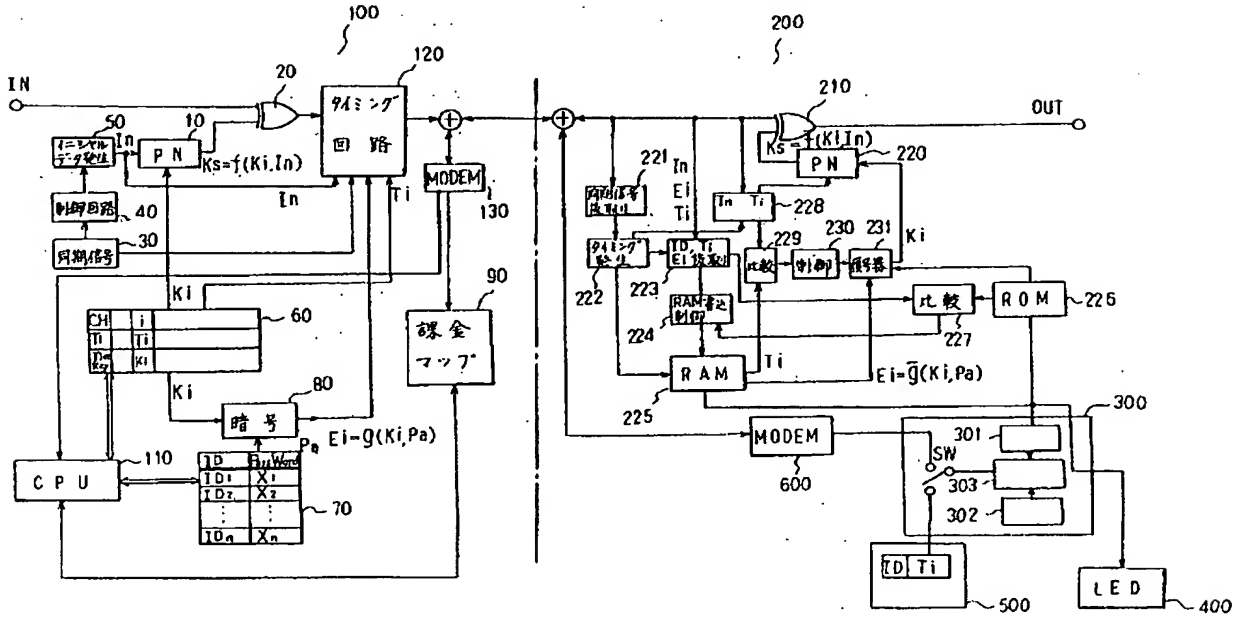
100…放送局側、　200…加入者側、
10…乱数発生手段、　20…スクランブル手段、
60,110…契約判別手段、60,70…データメモリ、
210…ディスクランブル手段、
229,230,231…鍵復号手段、
221,228,231…鍵抽出手段、
226,300,500…契約者識別手段。

代理人　弁理士　　則　近　憲　佑
（ほか1名）

第 1 図


100
IN
20
Ks=f(Ki,In)
90
課金
マップ
10
PN
CPU
110
Ki
Ti
In
60
70
200
210
OUT
Ks=f(Ks,In)
PN
220
ROM
226
RAM
225
CPU
300
500

第 2 図


100
IN
20
120
タイミング
回路
50
10
PN
Ks=f(Ki,In)
In
Ti
MODEM
130
制御回路
40
同期信号
30
Ki
60
90
課金
マップ
80
暗号
Ei=g(Ki,Pa)
CPU
110
70
200
210
OUT
Ks=f(Ki,In)
PN
220
221
In
Ei
Ti
228
229
230
231
222
223
224
225
RAM
ROM
226
227
Ei=g(Ki,Pa)
300
MODEM
600
301
SW
303
302
500
LED
400